

DII.COE.Final.SOL251.IP

**Defense Information Infrastructure (DII)
Common Operating Environment (COE)**

**Installation Procedures (IP) for
Courtney, version 1.0.0.2**

Document Version 1.0.0.2 revision 1

13 June 1997

Prepared for:

Defense Information Systems Agency

Prepared by:

**NRaD
San Diego, CA**

Table of Contents

1.	Scope	1
1.1	Identification	1
1.2	System Overview	1
2.	Referenced Documents	1
3.	System Environment	1
3.1	System Requirements	1
3.1.1	Hardware Requirements	1
3.1.2	Operating System Requirements	1
3.1.3	Kernel Requirements	1
3.2	System and Site Preparations	2
3.2.1	System Configuration	2
3.2.2	Operating System Preparation	2
3.2.3	Tape/Disk Preparation	2
4.	Installation Instructions	2
4.1	Media Booting Procedures	2
4.2	Installation Procedures	2
4.3	Installation of Upgrades	2
4.4	Installation Verification	2
4.5	Initializing the Software	3
4.6	List of Changes and Enhancements	3
4.7	Important Considerations	3
5.	Notes	3
	Appendix A.	3

This page intentionally left blank.

1. Scope

1.1 Identification

This Installation Procedures Document describes the installation procedures for Courtney (segprefix COURT) Version 1.0.0.2 for the Solaris 2.5.1 Platform.

1.2 System Overview

This version of Courtney monitors the network and identifies the source machines of SATAN probes/attacks. Courtney receives input from tcpdump counting the number of new services a machine originates within a certain window. If one machine connects to numerous services within that time window, Courtney identifies that machine as a potential SATAN host.

System configuration variables and command line options can be found in Appendix A of the SAM document for Courtney.

2. Referenced Documents

System Administrator's Manual (SAM) for Courtney version 1.0.0.2 revision 1, 13 June 1997.

3. System Environment

3.1 System Requirements

3.1.1 Hardware Requirements

None.

3.1.2 Operating System Requirements

The Sun/SPARC 2.5.1 Operating System is required to perform the installation of Courtney 1.0.0.2.

3.1.3 Kernel Requirements

DII COE Kernel Version 3.0.0.3 is required to perform the installation of Courtney 1.0.0.2.

3.2 System and Site Preparations

3.2.1 System Configuration

PERL Version 5 must be installed prior to installing Courtney 1.0.0.2. perl5 is available via anonymous FTP at the following site:

perl5 ftp.uu.net:/systems/gnu/perl5.001.tar.gz

3.2.2 Operating System Preparation

Log into the Sun/SPARC 2.5.1 system as “sysadmin.” After the system loads, go to the pull down menu labeled Software and select Segment Installer. This activates the COEInstaller.

3.2.3 Tape/Disk Preparation

Once the COEInstaller has been activated, choose the Select Source button to identify the source/location of the segment. When this window appears, select Other, then type in the location of your 8mm exabyte drive (which usually is /dev/rmt/0mn). Then choose OK.

4. Installation Instructions

4.1 Media Booting Procedures

None.

4.2 Installation Procedures

After completing paras 3.2.2 and 3.2.3 above, choose Read Contents in the Installer window to list the segments on the selected drive. The Courtney 1.0.0.2 segment will appear. Highlight the segment, then choose the Install button. This will install the Courtney segment into the /h/COE/Comp directory.

4.3 Installation of Upgrades

None.

4.4 Installation Verification

The installer script will verify that the segment has been installed. Two windows will pop up during installation. One will say “Courtney has been Installed.” The other will say “Courtney is running.”

Another way to verify that the segment has been installed is to go to the /h/COE/Comp directory to see if you see a COURT directory. If so, the segment has been installed.

4.5 Initializing the Software

To initialize the software, launch an xterm window. Log in as sysadmin, then su to root. At the root prompt, type

```
/h/COE/Comp/COURT/bin/courtney.pl &
```

This will activate Courtney 1.0.0.2.

By default, attacks will be logged via syslog at the “ALERT” logging level.

4.6 List of Changes and Enhancements

This version contains the conversion of Courtney from a COTS segment into a COE Component software segment.

This version contains a correction to the “Requires Descriptor” in the SegInfo file. The descriptor pointed to an incorrect version of PERL.

4.7 Important Considerations

None.

5. Notes

None.

Appendix A. Courtney INSTALL file.

Courtney INSTALL file located in data directory.

Here’s the quick way to get Courtney installed and running:

- 1) Get libpcap and tcpdump from ftp.ee.lbl.gov, patch them, and compile them according to their instruction files.
- 2) Get perl5 from ftp.uu.net and compile it according to its instructions.
- 3) As root, start Courtney with the command

```
./courtney.pl &
```

(located in /Seg_Home/bin)

By default, attacks will be logged via syslog at the “ALERT” logging level.

OSF/1 -- DIGITAL UNIX

“tcpdump: long jumps not supported”

Notes for running Courtney V1.2 on the Digital AXP under Digital UNIX.

To prevent tcpdump from dying with “tcpdump: long jumps not supported”:

- 1) Remove sunrpc and tcpmux or substitute their values.
These ports are not defined under Digital UNIX.
- 2) Remove
ports “1 or 10 or 100 or 1000 or 5000” and
ports “6001 or 6002 or 6010 or 6011 or 6012”
from the tcpdump filter. There must be too many options.

The following changes are shown below in the following courtney.pl code snippet.

FROM:

```
<open (TCPDUMP, “$tcpdump ‘\  
< (icmp[0] == 8) or \  
< (port sunrpc) or \  
< ((port (1 or 10 or 100 or 1000 or 5000 or 10000 or 20000 or 30000) or \  
< (port (6000 or 6001 or 6002 or 6010 or 6011 or 6012)) ) and \  
< (tcp[13] & 18 == 2) ) or \  
< (port (tcpmux or \  
< echo or \  
< discard or \  
< systat or \  
... other stuff ...
```

TO:

```
<open (TCPDUMP, “$tcpdump ‘\  
< (icmp[0] == 8) or \  
< ((port (10000 or 20000 or 30000) or \  
< (port (6000)) ) and \  
< (tcp[13] & 18 == 2) ) or \  
< (port (\br/>< echo or \  
< discard or \  

```

< systat or \
... other stuff ...